ID: 560435
Sample Name: Divit-RekutPO260122.exe
Cookbook: default.jbs
Time: 15:16:08
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

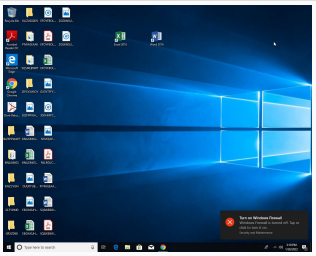
Windows Analysis Report

Divit-RekutPO260122.exe

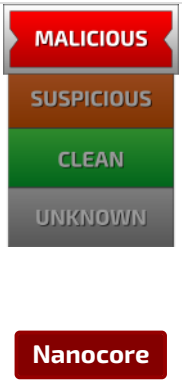
Overview

General Information

Sample Name:	Divit-RekutPO260122.exe
Analysis ID:	560435
MD5:	245ccd36af35ae…
SHA1:	0f224a20c017fd5..
SHA256:	d8c5e383bb522e..
Tags:	exe NanoCore RAT
Infos:	



Detection



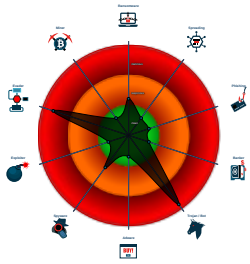
Nanocore

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Divit-RekutPO260122.exe (PID: 3928 cmdline: "C:\Users\user\Desktop\Divit-RekutPO260122.exe" MD5: 245CCD36AF35AE61D683A6F5CB2A8AE0)
  - powershell.exe (PID: 6880 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6816 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nUigecXuuIGz" /XML "C:\Users\user\AppData\Local\Temp\tmp4B31.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Divit-RekutPO260122.exe (PID: 6224 cmdline: C:\Users\user\Desktop\Divit-RekutPO260122.exe MD5: 245CCD36AF35AE61D683A6F5CB2A8AE0)
  - Divit-RekutPO260122.exe (PID: 6388 cmdline: C:\Users\user\Desktop\Divit-RekutPO260122.exe MD5: 245CCD36AF35AE61D683A6F5CB2A8AE0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "60bf7181-21f3-44c6-a8b6-9af1ea9b",
  "Group": "RR",
  "Domain1": "renareport.duckdns.org",
  "Domain2": "",
  "Port": 7522,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 3979,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 29994,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.568383321.0000000007620000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
0000000A.00000002.568383321.0000000007620000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
0000000A.00000002.568428902.0000000007640000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
0000000A.00000002.568428902.0000000007640000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
00000000.00000002.415807358.000000000328C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 62 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Divit-RekutPO260122.exe.57a0000.21.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
10.2.Divit-RekutPO260122.exe.57a0000.21.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
10.2.Divit-RekutPO260122.exe.7630000.29.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
10.2.Divit-RekutPO260122.exe.7630000.29.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
10.2.Divit-RekutPO260122.exe.7690000.34.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
Click to see the 164 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

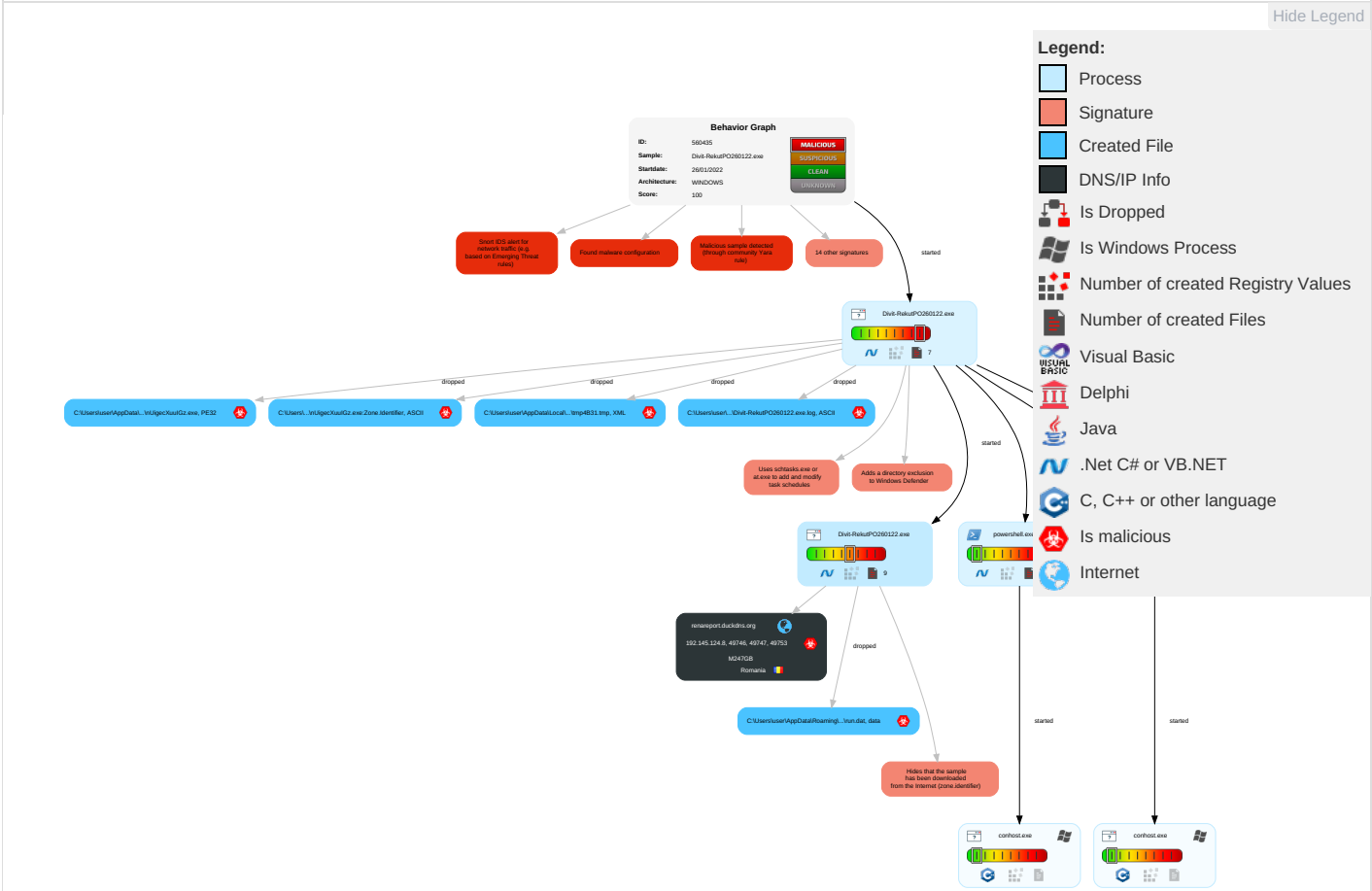
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 2 Process Injection	1 1 Masquerading	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

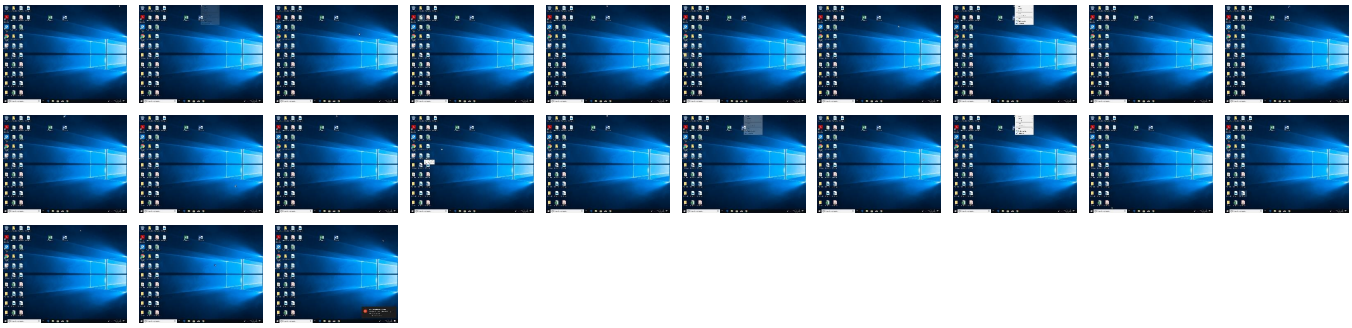
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Divit-RekutPO260122.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe	21%	ReversingLabs	Win32.Trojan.Worefflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.Divit-RekutPO260122.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Divit-RekutPO260122.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.Divit-RekutPO260122.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Divit-RekutPO260122.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Divit-RekutPO260122.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
10.2.Divit-RekutPO260122.exe.5a20000.22.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.0.Divit-RekutPO260122.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
renareport.duckdns.org	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
renareport.duckdns.org	192.145.124.8	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
renareport.duckdns.org	true	• Avira URL Cloud: safe	unknown

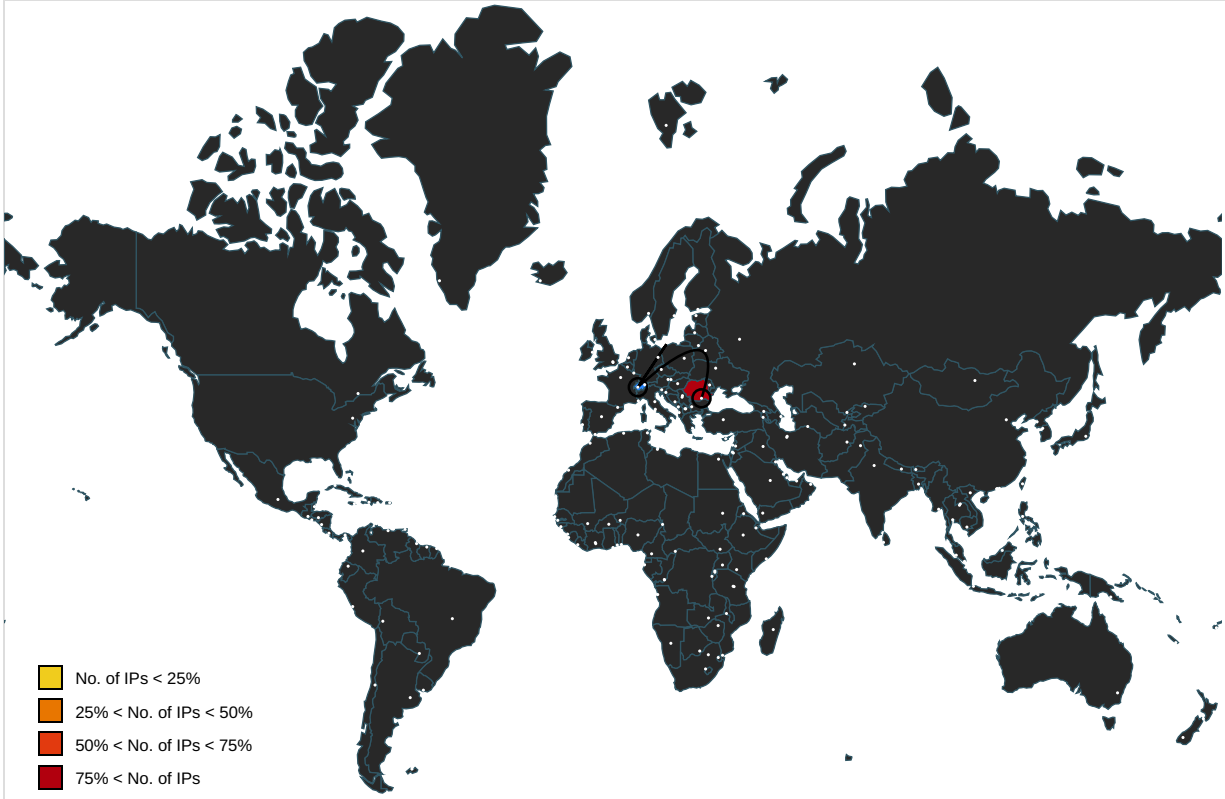
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.google.com/schemas/sitemap-video/1.1	Divit-RekutPO260122.exe, nUigecXuuIGz.exe.0.dr	false		high
http://www.fontbureau.com/designers/?	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	Divit-RekutPO260122.exe, 0000000A.00000002.563495687.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.565669120.0000000004B4F000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.565758830.0000000004C3A000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.568504011.0000000007650000.00000004.08000000.00040000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.565613381.0000000004AD9000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.561535124.000000000308D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sitemaps.org/schemas/sitemap/0.9_http://www.google.com/schemas/sitemap-image/1.1	Divit-RekutPO260122.exe, nUigecXuuIGz.exe.0.dr	false		high
http://www.carterandcone.coml	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sitemaps.org/schemas/sitemap/0.9	Divit-RekutPO260122.exe	false		high
http://fontfabrik.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sitemaps.org/schemas/sitemap/0.9T	Divit-RekutPO260122.exe, nUigecXuuIGz.exe.0.dr	false		high
http://www.jiyu-kobo.co.jp/	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.google.com/schemas/sitemap-image/1.1T	Divit-RekutPO260122.exe, nUigecXuuIGz.exe.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Divit-RekutPO260122.exe, 00000000.00000002.415807358.000000000328C000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 00000000.00000002.416031572.0000000003418000.00000004.00000800.00020000.00000000.sdmp, Divit-RekutPO260122.exe, 0000000A.00000002.561478044.0000000003021000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.google.com/schemas/sitemap-image/1.1	Divit-RekutPO260122.exe	false		high
http://www.sakkal.com	Divit-RekutPO260122.exe, 00000000.00000002.418260973.00000000072C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.145.124.8	renareport.duckdns.org	Romania		9009	M247GB	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560435
Start date:	26.01.2022
Start time:	15:16:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Divit-RekutPO260122.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/12@8/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1.3%) • Quality average: 60% • Quality standard deviation: 16.5%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Divit-RekutPO260122.exe, PID 6224 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:17:39	API Interceptor	497x Sleep call for process: Divit-RekutPO260122.exe modified
15:17:57	API Interceptor	26x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Divit-RekutPO260122.exe.log

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22292
Entropy (8bit):	5.60312134762376
Encrypted:	false
SSDEEP:	384:CtCDqC05lVpIlAJy0m9R8S0n0jultImv7Y9gxSJ3xGT1MavZlbAV7SbWX2NZBDIH:1lAJy0T0CltZfxcUC2fw2lVk
MD5:	F64CF9384302C37541ED741FC65FC9B6
SHA1:	C7775942A80C785791DA7C0AD89309AA486C3A6F
SHA-256:	0FCB201139E1B6C87DCA5D3F35260CAB4B96F739A1D41DD9864D0F37DE56387A
SHA-512:	58E572255E16230C431651AE7A8F35ECB9A984A2506BD47F0E771DE75C49E34AD430EA0545AFD259A0DC8305BE4E69E60E4470FA91DF7CA150A8C97EBF11F72B
Malicious:	false
Reputation:	low
Preview:	@...e.....|.....h.8./.&.#.....X...G.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gnay0xrg.ilv.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_j0zmopst.fpg.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp4B31.tmp

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.149653919067993
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLBxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTjv
MD5:	E16600EE6A875A8B0737F0A70A38DC3D
SHA1:	A341441B5C9FDABEA03FF87193F26D17087390DE
SHA-256:	9FDED473620F24395CE659827237B33C1054C701E77509F0C6DB2D287EE46646
SHA-512:	920094E8C5137D6C85B92CEA3DB1A9F7B43487BC7AE211C95EA8244657C4EEB341079085E6B6682B34A618C0FB8E5F52BB520337427A42726212ED33672C4B85
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028

SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:yHH:yHH
MD5:	05EB5D4610F76F1D181FD86857C7976A
SHA1:	B8B9BC39DBBE0490377D8E950ECE8B1BBD1B7267
SHA-256:	9D6416A9C1FAE0E85B03AC18EAAD7414B11E65EA6F1F7891B277A03842F24D61
SHA-512:	5C288C17375E8816024BFF3F7A0DDD77E3F96FC9EB957CA96B603A22FB5BF1864666E7A0C54897A92AF0AC3AA023497B232896DE2868F772594E7F6B23D3092D
Malicious:	**true**
Preview:	.K."..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_....Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v.""".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..l..oP=...xrK.?.............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i.........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	676864
Entropy (8bit):	7.330959464674909
Encrypted:	false
SSDEEP:	12288:HA6FTWVZtxD36OxOJUmjNA48bg/28PaDJHMBGeaa:HA/bN3xYUmfYtHeGFa
MD5:	245CCD36AF35AE61D683A6F5CB2A8AE0
SHA1:	0F224A20C017FD5FF1176804795F700756215C39
SHA-256:	D8C5E383BB522E41B0A95A2BBB051A5DE8B38F64297EBF78EA7C557067204F3E
SHA-512:	979B7D0C002BF3D88ABF8E1E5FB9E3875503E0E7FD6CBA7EE816B3D65249BB0DB9C77222B7511F8B6D9DBA53B66A4842AD044F127C7E3E26718092A9C679DFA5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(Q.a.....0..@.....^... ..`....@.. .....@.....^..O...`..... ....H.....text....>... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....R.....@..B.....^.....H.....`.....H.....&.(.....*...0..#.....,..r...ps!...z..(0...o"....*..0.....(0....+..*.0.....(#...(.... .+..*....0.....o$.....o%...io&....+..*...0..Q..... .....,5.....d...%...o'.....+.....e...o(...&..X....i2..+....e...o(...&*....0..z.....,....8d.....%o)....3...+o).....+.....,...8=.....,. (#.....o*...j.s+.....8.....o,.....%3....Xj./.....Xo,....%.....+.....

C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220126\PowerShell_transcript.745481.ulu11spy.20220126151755.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5797
Entropy (8bit):	5.404319122634798
Encrypted:	false
SSDEEP:	96:BZLhZNFqDo1ZWZuhZNFqDo1Z90+MjZVhZNFqDo1Z9FccwZb:r
MD5:	7B0082A46BFE3DE5ECB7E64204ACE49F
SHA1:	381AF56EFAD137E76C18613E563719AE489D4CA4
SHA-256:	0322BE800B4E13811F0FA8E7B2BCA698DD1DE47522A4AA5215E03102E0237836
SHA-512:	E98BC97FB6A17BE762B6E314A4691E705D77269B7086770811E82AD24B3230C3983B3FD52B1E8D857F2CDFC2EC4D09C726095C5B5D4CB21A7EF7788F6533980
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126151757..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 745481 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe..Process ID: 6880..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220126151757..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe..**********..Windows PowerShell transcript start..Start time: 20220126152137..Username: computer\user..RunAs User: computer\

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.330959464674909
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Divit-RekutPO260122.exe
File size:	676864
MD5:	245ccd36af35ae61d683a6f5cb2a8ae0
SHA1:	0f224a20c017fd5ff1176804795f700756215c39
SHA256:	d8c5e383bb522e41b0a95a2bbb051a5de8b38f64297ebf78ea7c557067204f3e
SHA512:	979b7d0c002bf3d88abf8e1e5fb9e3875503e0e7fd6cba7ee816b3d65249bb0db9c77222b7511f8b6d9dba53b66a4842ad044f127c7e3e26718092a9c679dfa5
SSDEEP:	12288:HA6FTWVZtxD36OxOJUmjNA48bg/28PaDJHMBGeaa:HA/bN3xYUmfYtHeGFa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(Q.a.....0..@.....^... ..`....@.. ....@.....

File Icon

Icon Hash:	c4c2c4dcf4c672bc

Static PE Info

General

Entrypoint:	0x495ed2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F15128 [Wed Jan 26 13:48:24 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x95e80	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0x10ef0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x93ed8	0x94000	False	0.761256862331	data	7.46826538838	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x10ef0	0x11000	False	0.131922104779	data	4.41817786213	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x96130	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xa6958	0x14	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa696c	0x396	big endian ispell hash file (?),		
RT_MANIFEST	0xa6d04	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	4.8.76.0
InternalName	KeyEventReco.exe
FileVersion	4.2.2.0
CompanyName	Destiny Realty Solutions
LegalTrademarks	
Comments	
ProductName	Markdown Editor Destiny Realty
ProductVersion	4.2.2.0
FileDescription	Markdown Editor
OriginalFilename	KeyEventReco.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-15:18:13.303284	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
01/26/22-15:18:13.571113	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	7522	192.168.2.3	192.145.124.8
01/26/22-15:18:23.633710	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
01/26/22-15:18:23.762963	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	7522	192.168.2.3	192.145.124.8
01/26/22-15:18:32.049511	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
01/26/22-15:18:32.189868	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	7522	192.168.2.3	192.145.124.8
01/26/22-15:18:41.556923	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
01/26/22-15:18:41.709556	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	7522	192.168.2.3	192.145.124.8
01/26/22-15:18:48.421970	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51143	8.8.8.8	192.168.2.3
01/26/22-15:18:48.575232	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	7522	192.168.2.3	192.145.124.8
01/26/22-15:18:55.373836	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	7522	192.168.2.3	192.145.124.8
01/26/22-15:19:04.470346	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52130	8.8.8.8	192.168.2.3
01/26/22-15:19:04.576292	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	7522	192.168.2.3	192.145.124.8
01/26/22-15:19:10.887268	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63297	8.8.8.8	192.168.2.3
01/26/22-15:19:10.991347	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	7522	192.168.2.3	192.145.124.8

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:18:13.314318895 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:13.418888092 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:13.418978930 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:13.571113110 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:13.728342056 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:13.765995979 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:13.888117075 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:13.990230083 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.058847904 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.201076984 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.235815048 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.381620884 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.381649017 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.381700993 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.381717920 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.381742954 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.381781101 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.381968021 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.382505894 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.382523060 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.382555008 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.382556915 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.382596970 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.382596970 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.382962942 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.383008003 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.483519077 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.483617067 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.483681917 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.483760118 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.483786106 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484122992 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484184980 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.484189987 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484251976 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484308958 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.484502077 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484553099 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.484569073 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484673977 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.484729052 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.485146999 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.485214949 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.485265970 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.485276937 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.485678911 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.485737085 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.485749006 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.485989094 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.486058950 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.486064911 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.486354113 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.486418962 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.486471891 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.486476898 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.489178896 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.585561991 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.585613966 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.585764885 CET	49746	7522	192.168.2.3	192.145.124.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:18:14.585789919 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.585830927 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.585900068 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.587991953 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588032961 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588097095 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.588432074 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588581085 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588762045 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588800907 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588823080 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.588840008 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.588880062 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588921070 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.588968992 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.589519024 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.589556932 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.589595079 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.589647055 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.589776039 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.589900017 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.590210915 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.590250015 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.590289116 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.590301991 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.590960979 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.591000080 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.591044903 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.591236115 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.591305017 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.591309071 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.591350079 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.591392994 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.591747046 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.592482090 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.592520952 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.592559099 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.592561007 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.592614889 CET	49746	7522	192.168.2.3	192.145.124.8
Jan 26, 2022 15:18:14.592737913 CET	7522	49746	192.145.124.8	192.168.2.3
Jan 26, 2022 15:18:14.593113899 CET	7522	49746	192.145.124.8	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:18:13.196201086 CET	54154	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:13.303283930 CET	53	54154	8.8.8.8	192.168.2.3
Jan 26, 2022 15:18:23.525368929 CET	52806	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:23.633709908 CET	53	52806	8.8.8.8	192.168.2.3
Jan 26, 2022 15:18:31.941472054 CET	64021	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:32.049510956 CET	53	64021	8.8.8.8	192.168.2.3
Jan 26, 2022 15:18:41.449799061 CET	60784	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:41.556922913 CET	53	60784	8.8.8.8	192.168.2.3
Jan 26, 2022 15:18:48.310863972 CET	51143	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:48.421969891 CET	53	51143	8.8.8.8	192.168.2.3
Jan 26, 2022 15:18:55.246186018 CET	56009	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:18:55.267179012 CET	53	56009	8.8.8.8	192.168.2.3
Jan 26, 2022 15:19:04.360207081 CET	52130	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:19:04.470345974 CET	53	52130	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 15:19:10.777728081 CET	63297	53	192.168.2.3	8.8.8.8
Jan 26, 2022 15:19:10.887268066 CET	53	63297	8.8.8.8	192.168.2.3

DNS Queries

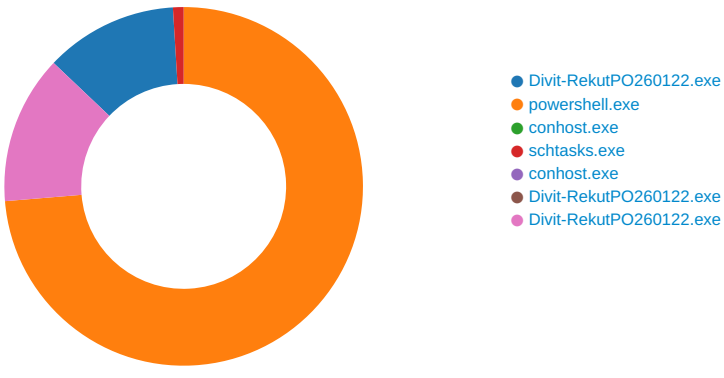
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 15:18:13.196201086 CET	192.168.2.3	8.8.8.8	0x74d9	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:23.525368929 CET	192.168.2.3	8.8.8.8	0xc690	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:31.941472054 CET	192.168.2.3	8.8.8.8	0x5a71	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:41.449799061 CET	192.168.2.3	8.8.8.8	0xba48	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:48.310863972 CET	192.168.2.3	8.8.8.8	0xa619	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:55.246186018 CET	192.168.2.3	8.8.8.8	0xaa6e	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:19:04.360207081 CET	192.168.2.3	8.8.8.8	0x4a77	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)
Jan 26, 2022 15:19:10.777728081 CET	192.168.2.3	8.8.8.8	0xee9b	Standard query (0)	renareport .duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 15:18:13.303283930 CET	8.8.8.8	192.168.2.3	0x74d9	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:23.633709908 CET	8.8.8.8	192.168.2.3	0xc690	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:32.049510956 CET	8.8.8.8	192.168.2.3	0x5a71	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:41.556922913 CET	8.8.8.8	192.168.2.3	0xba48	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:48.421969891 CET	8.8.8.8	192.168.2.3	0xa619	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:18:55.267179012 CET	8.8.8.8	192.168.2.3	0xaa6e	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:19:04.470345974 CET	8.8.8.8	192.168.2.3	0x4a77	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)
Jan 26, 2022 15:19:10.887268066 CET	8.8.8.8	192.168.2.3	0xee9b	No error (0)	renareport .duckdns.org		192.145.124.8	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Divit-RekutPO260122.exe PID: 3928, Parent PID: 3248

General

Target ID:	0
Start time:	15:17:06
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Divit-RekutPO260122.exe"
Imagebase:	0xe20000
File size:	676864 bytes
MD5 hash:	245CCD36AF35AE61D683A6F5CB2A8AE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.415807358.000000000328C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.416450713.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.416450713.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.416450713.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.416031572.0000000003418000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6D6ADD66	CopyFileW
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6D6ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4B31.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D6A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Divit-RekutPO260122.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6EB6C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4B31.tmp	success or wait	1	6D6A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 28 51 fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 40 09 00 00 12 01 00 00 00 00 00 fd 5e 09 00 00 20 00 00 00 60 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0a 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL(Qa0@^ `@ @	success or wait	3	6D6ADD66	CopyFileW
C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6D6ADD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4B31.tmp	0	1599	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationInfo>	success or wait	1	6D6A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Divit-RekutPO260122.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EB6C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E83CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile

Analysis Process: powershell.exe PID: **6880**, Parent PID: **3928**

General

Target ID:	5
Start time:	15:17:54
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nUigecXuuIGz.exe
Imagebase:	0x1290000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0zmopst.fpg.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gnay0xrg.ilv.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW
C:\Users\user\Documents\20220126	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6ABEFF	CreateDirectoryW
C:\Users\user\Documents\20220126\PowerShell_transcript.745481.uIu11spy.20220126151755.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0zmopst.fpg.ps1	success or wait	1	6D6A6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gnay0xrg.ilv.psm1	success or wait	1	6D6A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_j0zmopst.fpg.ps1	0	1	31	1	success or wait	1	6D6A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_gnay0xrg.ilv.psm1	0	1	31	1	success or wait	1	6D6A1B4F	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.745481.uIu11spy.20220126151755.txt	0	3	ff		success or wait	1	6D6A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.745481.uIu11spy.20220126151755.txt	3	679	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 31 35 31 37 35 37 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 34 35 34 38 31 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220126151757Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 745481 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6D6A1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 7c 14 00 00 1a 00 00 00 68 0d 38 04 2f 09 26 09 23 09 00 00 fd 00 58 00 08 00 47 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e|h8/&#XG@	success or wait	1	6EB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 52 00 00 00 0e 00 20 00	H<@^L"My:R	success or wait	17	6EB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6EB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6EB276FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6EB276FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40	T@>@g@@@@V@H@X@[@NT@HT@S@S@hT@ S@S@S@\@T@T@@X@? X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@ M@!M@;M@D@D @@M@<M@$M@8M@? M@;@;@;@<@<@<@W@M@E@	success or wait	11	6EB276FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E83CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E83CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E83CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E835705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E841F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23204	success or wait	1	6E84203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E7903DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	135	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D6A1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E7903DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E835705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	13	6D6A1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6D6A1B4F	ReadFile

Analysis Process: conhost.exe PID: **6884**, Parent PID: **6880**

General

Target ID:	6
Start time:	15:17:54
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **6816**, Parent PID: **3928**

General

Target ID:	7
Start time:	15:17:55
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nUigecXuuIGz" /XML "C:\Users\user\AppData\Local\Temp\tmp4B31.tmp
Imagebase:	0x2b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4B31.tmp	unknown	2	success or wait	1	2BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4B31.tmp	unknown	1600	success or wait	1	2BABD9	ReadFile

Analysis Process: conhost.exe PID: **1364**, Parent PID: **6816**

General

Target ID:	8

Start time:	15:17:56
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Divit-RekutPO260122.exe PID: **6224**, Parent PID: **3928**

General

Target ID:	9
Start time:	15:17:57
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Imagebase:	0x390000
File size:	676864 bytes
MD5 hash:	245CCD36AF35AE61D683A6F5CB2A8AE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Divit-RekutPO260122.exe PID: **6388**, Parent PID: **3928**

General

Target ID:	10
Start time:	15:17:58
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Divit-RekutPO260122.exe
Imagebase:	0xd40000
File size:	676864 bytes
MD5 hash:	245CCD36AF35AE61D683A6F5CB2A8AE0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568383321.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568383321.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568428902.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568428902.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.410999862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.410999862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.410999862.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.561478044.0000000003021000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568664652.00000000076E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568664652.00000000076E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568120467.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568120467.0000000007340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.566728475.00000000057A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.566728475.00000000057A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.565669120.0000000004B4F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568184518.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568184518.0000000007350000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568608107.00000000076A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568608107.00000000076A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568316607.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568316607.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.566773254.0000000005A20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.566773254.0000000005A20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.566773254.0000000005A20000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.563495687.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.563495687.0000000004908000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568504011.0000000007650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568504011.0000000007650000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.559962462.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.559962462.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.559962462.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568398477.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568398477.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.406664976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.406664976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.406664976.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.412369775.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.412369775.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.412369775.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568524789.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568524789.0000000007660000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568590843.0000000007690000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568590843.0000000007690000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.565758830.0000000004C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.565758830.0000000004C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.411830599.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.411830599.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.411830599.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.563057311.0000000004059000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.563057311.0000000004059000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.568548705.0000000007670000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.568548705.0000000007670000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.565613381.0000000004AD9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.565613381.0000000004AD9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.561535124.000000000308D000.00000004.00000800.00020000.00000000.sdmp,

	Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E85CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6ABEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6ABEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D6ABEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	6	6D6A1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D6A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Divit-RekutPO260122.exe:Zone.Identifier	success or wait	1	6D622935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	c8 4b 1d 22 fd fd 48	K"H	success or wait	1	6D6A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	8	6D6A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6D6A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6D6A1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E835705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E83CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E7903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E7903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E835705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D6A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D6A1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Divit-RekutPO260122.exe	unknown	4096	success or wait	1	6E81D72F	unknown
C:\Users\user\Desktop\Divit-RekutPO260122.exe	unknown	512	success or wait	1	6E81D72F	unknown

Disassembly

No disassembly